OT & CYBERSECURITY CONFERENTIE

22 April 2026 • Amersfoort

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

EVEN VOORSTELLEN

- Rob Hulsebos, 1961
- Beroep: techneut, werkzaam in OT (voordat het begrip bestond)
  - Softwareontwikkelaar embedded- en real-time systemen
  - Machinebouwer
  - Industrieel-netwerk troubleshooter
  - Nu bij Forescout (Eindhoven)
- Daarnaast docent, trainer, freelance journalist, deeltijd-zzp'er, ...

OT & CYBERSECURITY CONFERENTIE

FORESCOUT EINDHOVEN

- Ex “Security Matters”
- OT Competence Center in Ehv
- VedereLabs research
- Ontwikkelhub eyeInspect (OT Intrusion Detection System)
  - Threat Detection
  - Asset Lifecycle Management
  - **Vulnerability Management**

OT & CYBERSECURITY CONFERENTIE

STELLING

Waarom leveranciers een betere bron zijn voor informatie over kwetsbaarheden in OT producten dan de NVD en CISA

(Voordracht op persoonlijke titel)

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

PATCH MANAGEMENT

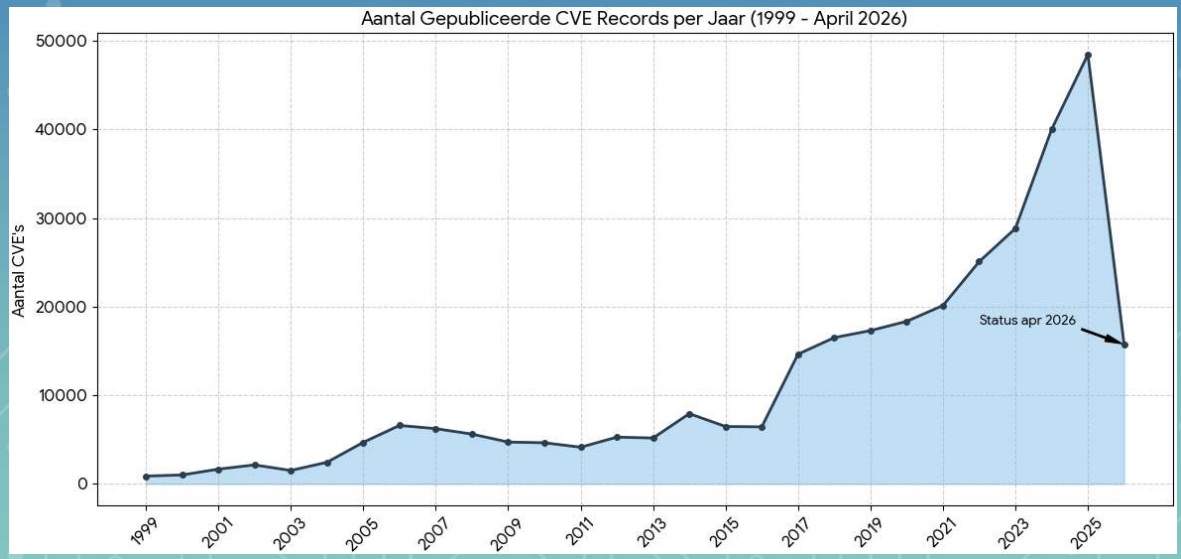
- Vereist in elke cybersecurity standard (b.v. IEC 62443-2-3)
- Gegeven een asset-register / CMDB …
  - Zoek uit: elke kwetsbaarheden zijn bekend geworden
  - Selecteer: welke daarvan zitten er in ***mijn*** systeem ?
- Automatische / handmatige uitvoering afhankelijk van (meta)data
  - “Handtekening” van device -> leverancier, model, software versie

    versus…
  - Wat is genoemd in de rapportage (vendor advisory)

OT & CYBERSECURITY CONFERENTIE

EEN STUKJE CVE+NVD GESCHIEDENIS

- Behoefte om centrale database voor kwetsbaarheden te hebben
- CVEs sinds 1999
- “National Vulnerability Database” (NVD) sinds 2005
- In zoverre ‘National’ dat de hele wereld hier zijn kwetsbaarheden in publiceert
- Enorme groei sinds 2021 (extra sinds 2024 vanwege Linux kernel, ca. 10 per dag)



DE WERELD IS VERANDERD

- Steeds meer CVEs (> *100 per dag*)
- Handmatig werk is niet schaalbaar; er zijn nu hulptroepen (CNAs)
- Eén CVE kan honderden producten / sw versies omvatten
- Voor automatische verwerking is meer nodig dan tekst
  - Is deze CVE van toepassing op *mijn* asset?
  - Dit is een moeilijk automatiseerbaar probleem
  - Poging met ‘CPEs’

CVE EVOLUTIE

- 10 jaar geleden: één kwetsbaarheid -> één product / softwareversie
- Vandaag kan één kwetsbaarheid ...
  - ... meerdere product*families* omvatten, met honderden producten
  - ... van verschillende leveranciers
  - ... tientallen tot duizenden getroffen softwareversies noemen
  - ... waarvan sommige out-of-support zijn / of al fix hebben / of nog fix krijgen
  - En dan nog in verschillende combinaties
- Dat is te breed om in een CVE te administreren (CVSS, CPEs)
  - Die ook niet wordt geupdate
  - Bijvoorbeeld: op moment van publicatie “Alle versies zijn kwetsbaar”
    Is dat een tijdje later ook nog zo? -> false positives

VERRIJKING

- Na nieuwe CVE:
  - NVD (of externe) analyst voegt verrijking toe op basis van publieke gegevens
- Wat zien we daarbij soms:
  - Andere opvattingen over waarde van de CVSS (kan daardoor wijzigen van status ‘Critical/High’ -> ‘Medium’
  - Meerdere afwijkende CVSS is verwarrend voor eindgebruikers
  - Niet altijd diepgaand inzicht in betroffen software / hardware
  - Soms lijkt de analyst meer te weten dan de leverancier zelf (???)
  - Vaak typo’s (vervelend in matching van sw versies)
- Heranalyse ook bij anderen te zien

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD — N/A — NVD assessment not yet provided.

CNA: ICS-CERT — **CVSS-B** 7.0 HIGH — **Vector:** CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/S

EUVD-2025-203181

Severity	Alternative IDs
CVSS Base Score: 7 (v4.0) (CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/SC:N/	GHSA-vjcx-2xxh-mc9h CVE-2025-13970

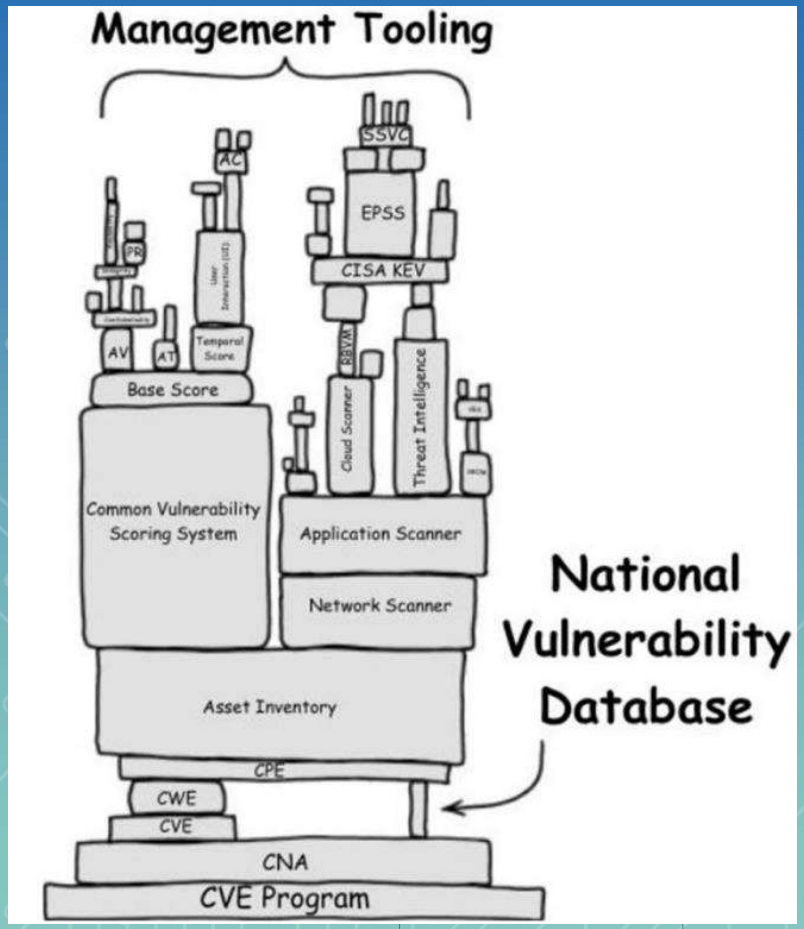
- OpenPLC_V3 vers:all/* (CVE-2025-13970, CVE-2026-28205, CVE-2026-35556, CVE-2026-35063)

CVSS	Vendor	Equipment	Vulnerabilities
v3 8.9	OpenPLC_V3	OpenPLC_V3 (Update A)	Cross-Site Request Forgery (CSRF),

OT & CYBERSECURITY CONFERENTIE

NVD ISSUES IN 2024 EN 2025

- 2024: Massale achterstand in zgn. ‘verrijking’ van nieuwe CVEs
  - Budgetproblemen en minder mankracht
  - Maar wel 30% meer CVEs
  - Verrijking: CVSS score bepalen, CPEs toevoegen (metadata)
  - Geen verrijking? Problemen voor supply-chain tools!
- 2025: Budget op
  - Dreigende totale uitval van gehele NVD
  - Laatste-minuut redding, noodbudget tot 2026
  - “Toevallig” komt diezelfde avond de EUVD in de lucht
- 2026: Structurele lange-termijn oplossing is er
  - Toch nog steeds ca. 31000 CVEs in de wachtrij voor verrijking



OT & CYBERSECURITY CONFERENTIE

NOG STEEDS ACHTERSTAND

CVE-2025-40944 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

3 maanden al

Description

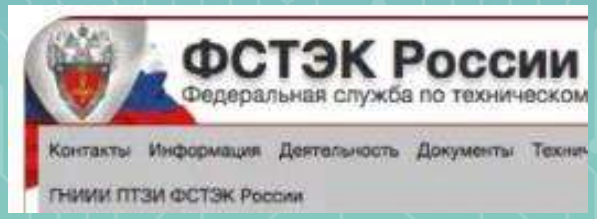
A vulnerability has been identified in SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0) (All versions), SIMATIC ET 200MP IM 155-5 PN (6ES7155-5AA00-0AC0) (All versions >= V4.2.0), SIMATIC ET 200SP IM 155-6 MF HF (6ES7155-6MU00-0CN0) (All versions), SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants) (All versions < V1.3), SIMATIC ET 200SP IM 155-6 PN R1 (6ES7155-6AU00-0HM0) (All versions < V6.0.1), SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0) (All versions >= V4.2.0), SIMATIC ET 200SP IM 155-6 PN/3 HF (6ES7155-6AU30-0CN0) (All versions < V4.2.2), SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0) (All versions), SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0) (All versions < V6.0.0), SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0) (All versions >= V4.2.0), SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0) (All versions >= V4.2.0), SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-2CN0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-7CN0) (All

QUICK INFO

CVE Dictionary Entry:
CVE-2025-40944
NVD Published Date:
01/13/2026
NVD Last Modified:
01/13/2026
Source:
Siemens AG

ZITTEN WE DAN VAST AAN DE NVD ?

- Er zijn nog veel andere bronnen met kwetsbaarheidinformatie
  - CISA (ex ICS-CERT), VDE-CERT, JP-CERT, NCSC, EUVD, FSTEC, CNCERT, CNNVD, GHSA ...
  - Hiervan hebben alleen CISA en VDE-CERT een specifieke OT-focus
- Wel veel copy/paste heen-en-weer



OT & CYBERSECURITY CONFERENTIE

CISA VOOR OT KWETSBAARHEDEN

- ICS-CERT startte in 2009, specifiek voor OT kwetsbaarheden
  - Leveranciers deden toen nauwelijks iets
  - Goede bron (vroeger: enige bron) van informatie voor OT asset owners
- Eigen advisories (zoek op ID: ICSA-yyyy-ddd-nn)
- 508 ICSA's in 2025 (vergelijk met 48K CVE's) 423 in 2024, 380 in 2023

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

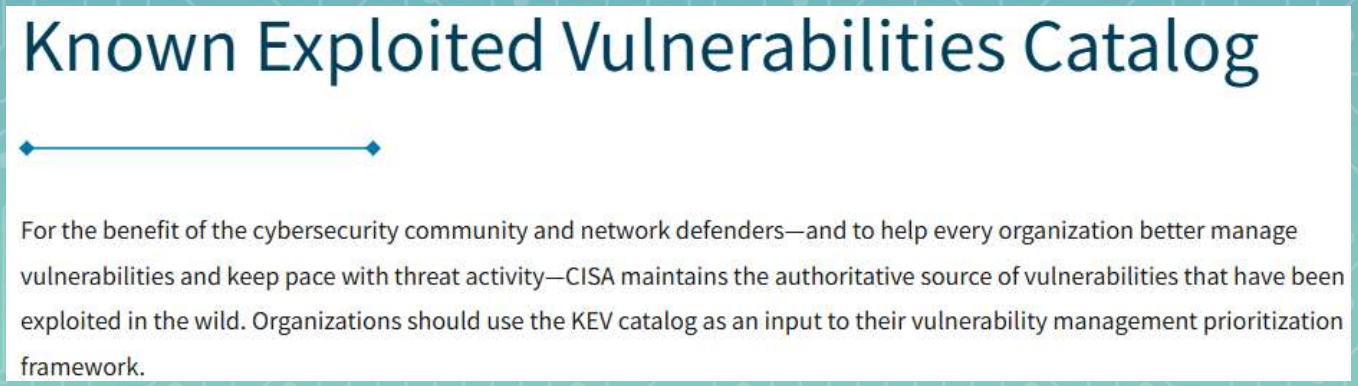
WAT IS ER *NIET* OP CISA ?

- Veel OT kwetsbaarheden zijn ***niet*** op CISA te vinden
  - Hangt vaak af van welwillendheid leverancier
- Updates van leveranciers komen vaak niet (meer) door
- Recente revamp van website verwijst niet meer naar leveranciers
- *Persoonlijk vind ik nut van CISA sterk afgenomen*

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global).

OOK CISA: KEV

- “Known Exploited Vulnerabilities”
- Kwetsbaarheden waarvan exploitability bekend is
- Waarom tijd besteden aan CVEs waar niemand interesse in heeft?



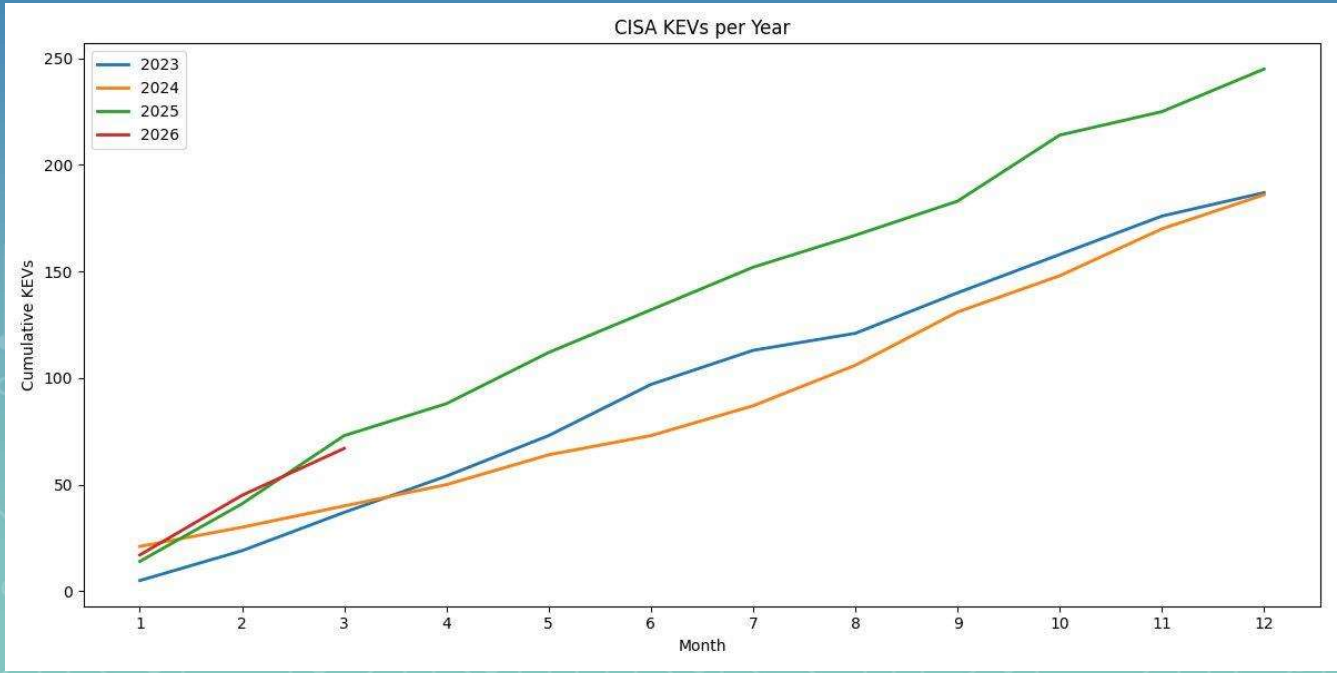
Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

OT & CYBERSECURITY CONFERENTIE

LET OP: GEEN CVE ? DAN OOK GEEN KEV

- KEVs zijn nuttig voor het prioriteren van vuln’s
- Ca. 250 per jaar
- Maar: **kan alleen als er een CVE is**
- Idem voor EPSS



OT & CYBERSECURITY CONFERENTIE

HOE KAN DE LEVERANCIER HELPEN

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

HOE HELPT DE LEVERANCIER

- Publiceren advisories (met of zonder CVE, liefst mét)
  - Ervaring: hier is nog ***veel*** verbetering mogelijk
- Goede uitleg wat de getroffen producten zijn
- Oppikken advisories van onderzoekers (coordinated disclosure)
  - Kom vaak veel wantrouwen tegen
- Analyseren van supply-chain issues
  - Volgt dan nieuwe advisory (meestal zonder CVE, of onder *dezelfde* CVE ☹)

GETROFFEN PRODUCTEN

- Wat in een advisory staat, is vaak iets anders dan op het netwerk
  - B.v. advisory zegt: PLC type “Rockwell MicroLogix V32.010” is getroffen
  - Op network te zien: ik ben een “1766-L32BXBA V33.011”
- Vertaalslag is nodig
  - Welke modellen zijn allemaal een MicroLogix? En welke niet?
  - Zit de bug in V32.010 ook in V33.011 ? (hangt af van sw-trains)
- Dit poogde de NVD op te lossen met CPEs, maar is niet dekkend genoeg
  - En als ze al kloppen, dan alleen op moment van publicatie
  - Leveranciers zelf hebben dit nog niet
- **Leverancier kent zijn eigen producten uiteraard**

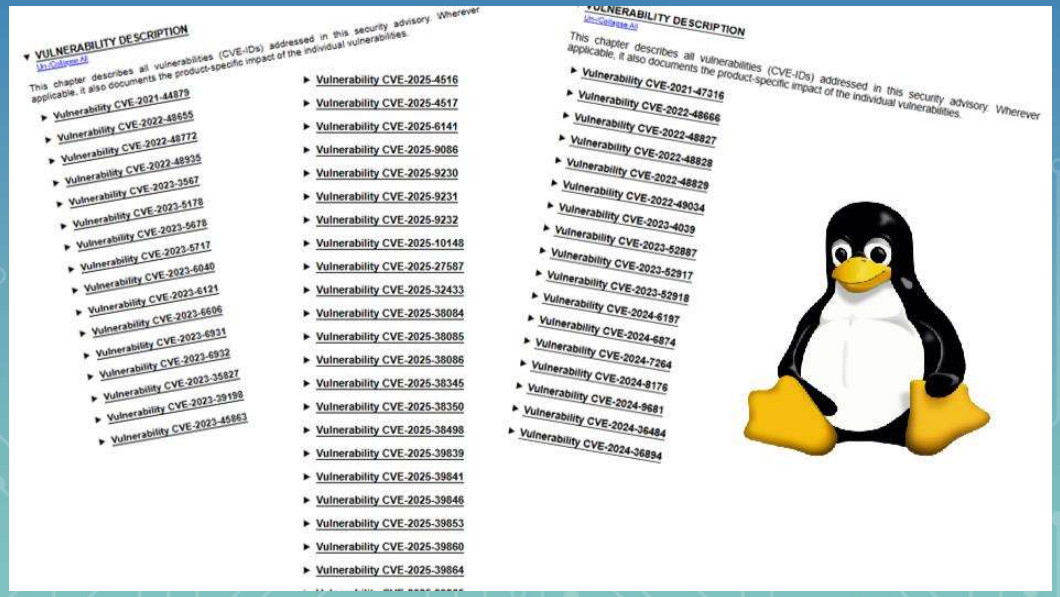
LACUNES IN INDIVIDUELE CVEs

- Scenario: onderzoeker vindt een kwetsbaarheid in een product
- Registreert een nieuwe CVE
  - Noemt enkel het product op zijn/haar bureau
  - Eén hardware variant, één software versie Vx.y
- Maar:
  - Zijn er nog meer producten van die leverancier (in een familie) ?
  - Zit de kwetsbaarheid ook in eerdere sw versies (vóór Vx.y) ? Of niet?
- **Enkel de leverancier weet dit**
  - Vulnerability disclosure moet via leverancier lopen!

OT & CYBERSECURITY CONFERENTIE

VERRIJKING SUPPLY-CHAIN OPWAARTS

- NVD voert geen opwaartse supply-chain analyse uit (in welke producten zit *deze* kwetsbaarheid)
- Voorbeeld:
  - Kwetsbaarheid in Linux kernel K
  - Product P gebruikt K
  - Iets terug te vinden in CVE ? Nee!
- **Leverancier van P is nodig!**
  - Soms volgt hier een nieuwe CVE
  - Soms niet! -> zie leverancier P website
- Wat gaat de CRA hier doen?



Bron: Siemens SSA-613316, SSA-355557, SSA-089022 welke resp. 351, 501 en 51 CVEs bevatten.

WAT! GEEN CVE ?

- Helaas, sommige leveranciers doen niet aan CVEs
  - Want: niet verplicht
  - Hooguit publicatie van advisory op eigen website
  - En soms enkel naar nationale CERT
- Soms wordt CVE uitgetrokken, maar niet ingevuld
- Voor het ecosysteem bestaan zulke kwetsbaarheden dan niet
  - Niet te vinden in NVD-gebaseerde vulnerability-management tools
  - Asset wordt dan niet als kwetsbaar gesignaleerd

Hi!
I forwarder your question to our Security Team and they send me the following statment:

"Requesting a CVE ID is not mandatory. We evaluate the need for a CVE ID on a case-by-case basis"

I hope this answers your questions sufficiently.

With Kind regards

_____

[redacted]
Support Engineer

LEVERANCIERS INFORMATIE

- Véél gebruikelijker dan enkele jaren geleden (werpt de CRA zijn schaduw vooruit ?)
- Sommige leveranciers volgen “Patch Tuesday” cyclus (á la Microsoft)
- Niet alles is (helaas) openbaar
  - Bv alleen voor geregistreerde klanten, of product-eigenaren

IS ALLES PERFECT ?

- NVD heeft API (+), maar leveranciers veelal niet (-)
- Geen gestandaardiseerde (machine-leesbaar) formaat
  - PDF, TXT, HTML ...
- Wél machine-readable formaat: CSAF
  - Common Security Advisory Format
  - Steeds gangbaarder, maar kan veel beter!
- Maar dan ook graag zonder restrictieve licenties

KAN HET NOG BETER ?

- Publicatie van advisories wordt vaak geschuwd (reputatieverlies, geen coordinated disclosure, angst voor … ?)
- Discussies a la “dit is geen bug maar een feature”
- Geeft werk ?
- Vertragingen bij afhandeling / correspondentie
- PSIRT / CERT kent eigen producten niet

- Diverse OT-leveranciers geven al het goede voorbeeld!

ADVIES: LEVERANCIERS EERST

- Controleer advisories van eigen leveranciers eerst
  - Eerder, nauwkeuriger, uitgebreider
  - Supply-chain afhankelijkheden zijn hen bekend
- Leveranciers die **niets** publiceren ?
  - Onmogelijk eigenlijk, waarom ?
  - Misschien stilletjes geïntegreerd samen met een functionele update?
  - Ga discussie aan, zeker n.a.v. aankomende CRA wetgeving

CONCLUSIE: LEVERANCIER IS NODIG

- Beste kwaliteit informatie over kwetsbaarheden
  - Het betreft *zijn* producten, wie kan het beter weten?
  - Meest accuraat
  - Krijgt updates door
  - Sneller beschikbaar
  - Omvat productlijnen / alle software versies
  - Kent supply-chain
- NVD blijft nodig als ecosysteem-infrastructuur

EN DAN NOG EVEN DIT...

3.1 Introduction

Claude Mythos Preview is the most cyber-capable model we have released, surpassing all previous models across our internal evaluation suite and saturating nearly all of our existing internal and known external capability evaluations. As model capabilities have

In response to the improvements in cyber capabilities, we have elected to restrict access to the model, prioritizing industry and open-source partners who will be using Claude Mythos Preview to help secure their systems through Project Glasswing. We are also continuing to improve and deploy enhanced mitigations (including monitoring and detection capabilities) to enable rapid response to cyber misuse, as outlined below.

OT & CYBERSECURITY CONFERENTIE

DANK VOOR UW AANDACHT

rob.hulsebos@forescout.com

www.linkedin.com/in/rob-hulsebos